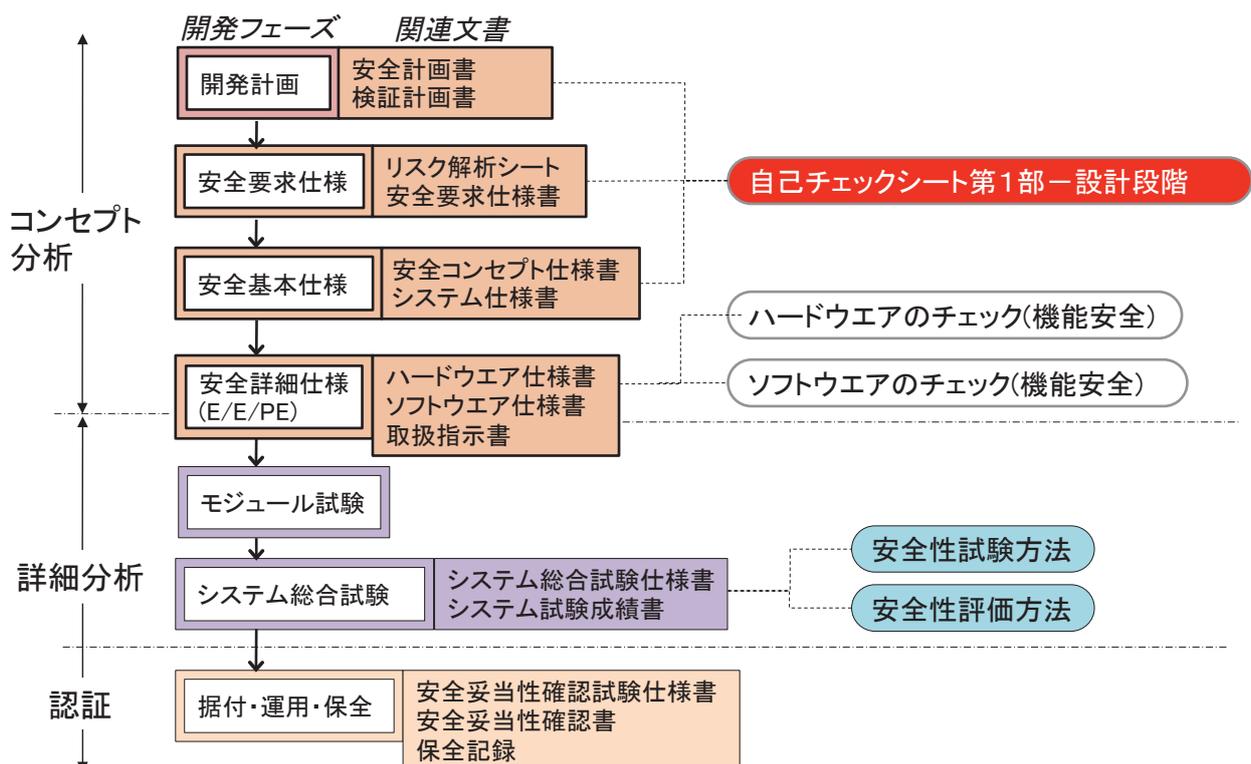
安全コンセプトチェックシートの概要

安全WG
(独)労働安全衛生総合研究所　池田博康

チェックシート第1部ー設計段階の目的と概要

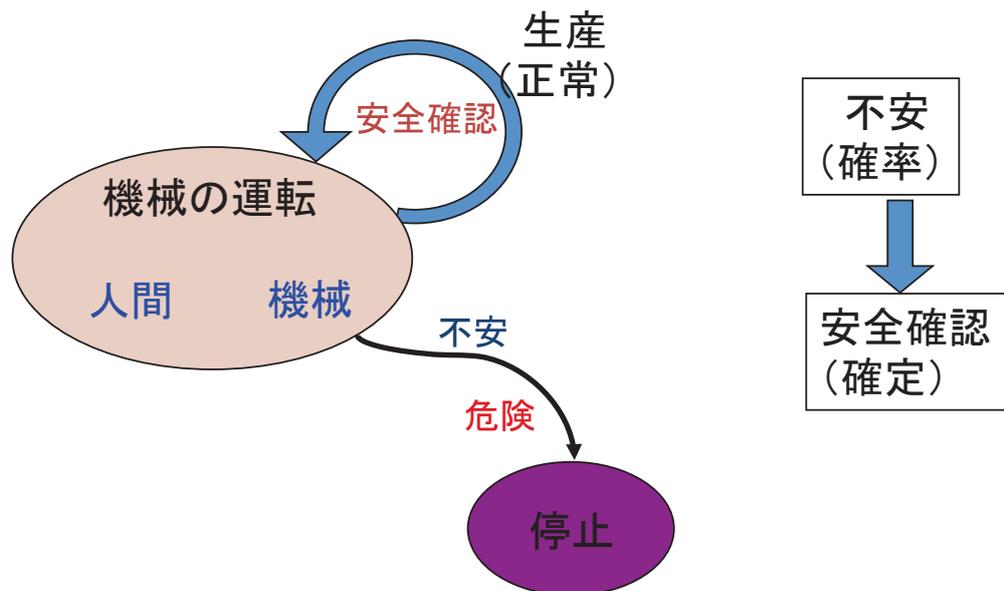
目的：ロボット介護機器の設計・開発段階で(機能)安全計画書、安全コンセプト・システム・安全要求仕様書を作成する場合の必要事項を自己チェックする

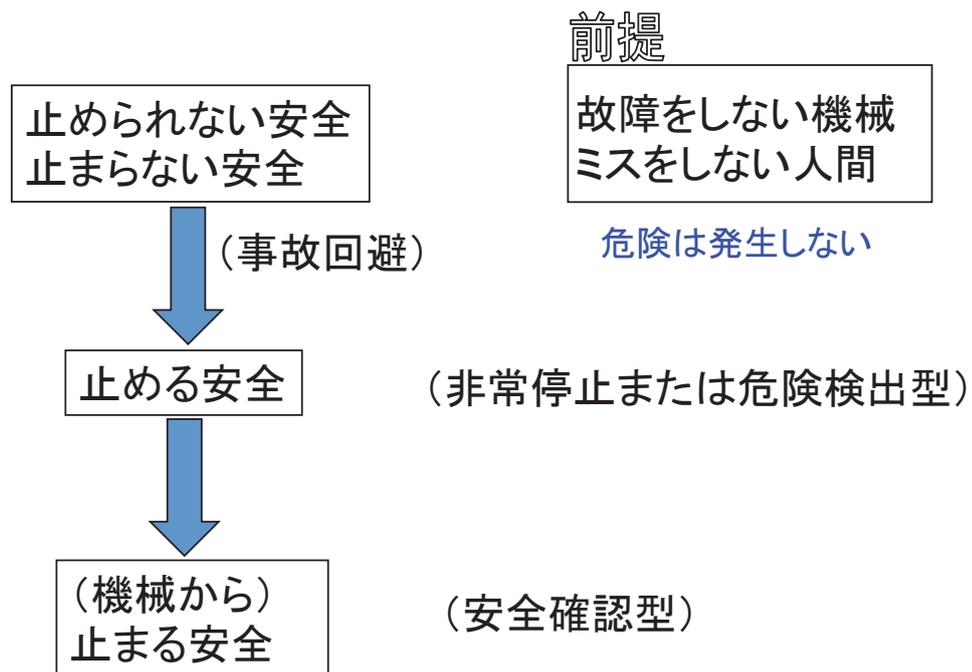
位置付け：安全コンセプト認証を念頭においたコンセプト分析内容と必要文書の確認

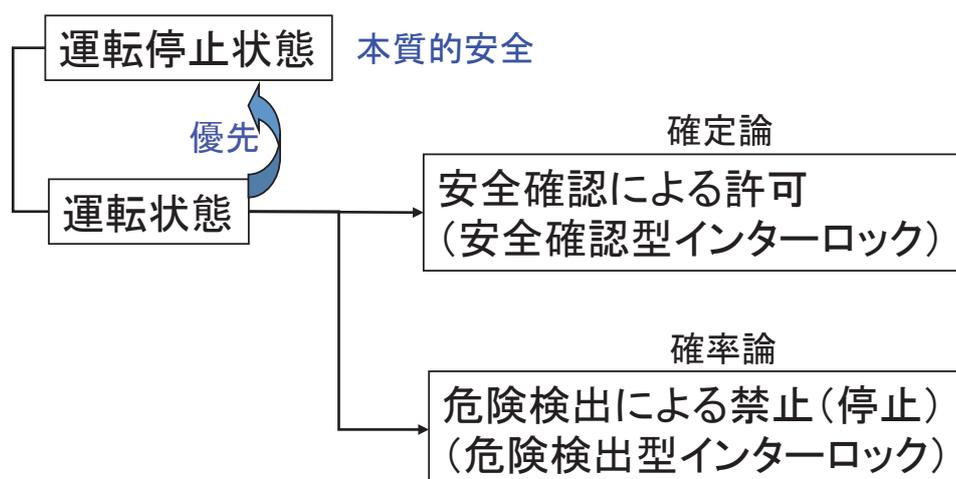
チェック方法：6大項目の下の59設問毎に、それが実施済み又は取組中であるか否かを自己チェックし、大項目毎の達成度(満足度)を判断

各対象機器の優劣ではなく、安全設計において弱点を明確化する
製品製造の段階まで想定する

2つの安全状態

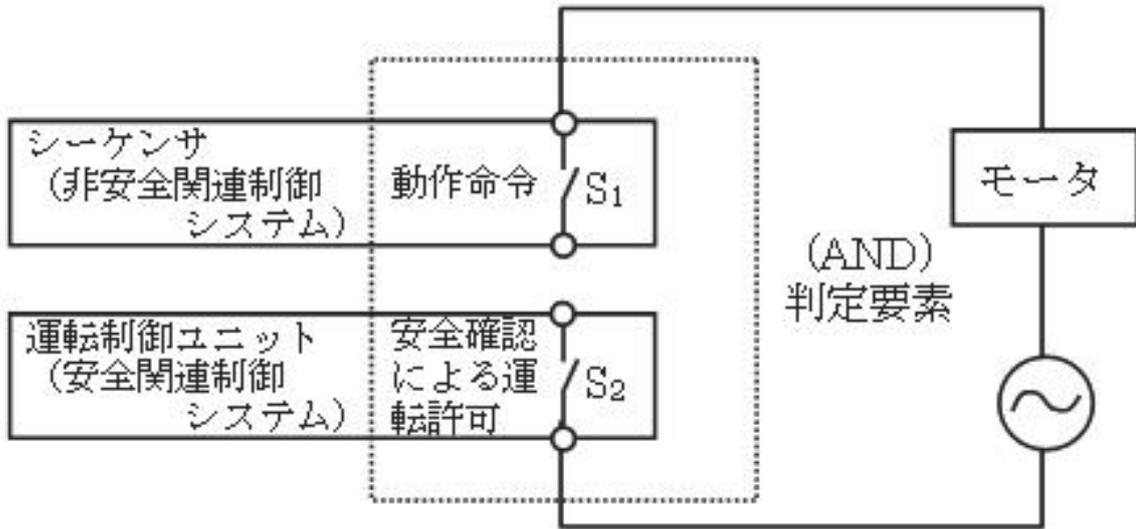
安全基礎知識

○合目的的安全状態(安全が確認されて運転中)
○無条件安全状態(機械の運転停止状態)

止まる安全

安全基礎知識

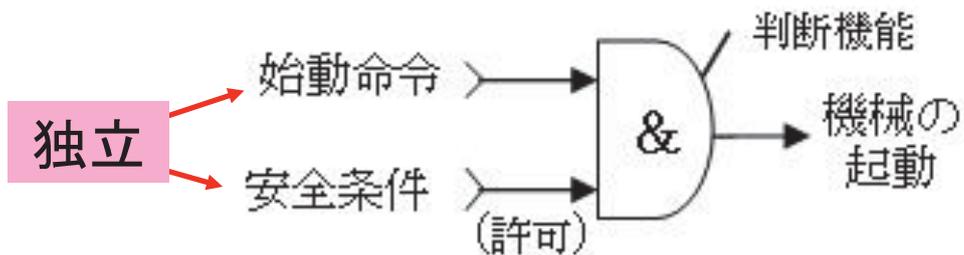
安全状態の優先性

安全基礎知識

安全が確認できないときは停止

独立性の確保

安全基礎知識

分離はコスト面でも有利

独立性の確保

安全基礎知識

安全条件

外部の安全条件の場合

安全位置、安全状態

機能的安全性

安全機能の診断、ソフトでの安全性の確認

チェックシートの設問趣旨と対応安全規格類(1)

開発の基本的考え方

No	設問項目	趣旨	対応規格
Ⅰ	ロボット介護機器の形態	ロボットの型の分類	JIS B9705-1:2011(4)
	安全設計方針	安全設計コンセプト･方針の確認 安全仕様の確認	
	人とロボット介護機器の役割	危険事象への対応(検知、回避を含む)の主体の確認	

チェックシートの設問趣旨と対応安全規格類(2)

リスクアセスメントのPDCA状況

No	設問項目	趣旨	対応規格
Ⅱ	リスクアセスメント基準	準拠している規格･基準の確認	JIS B 9700:2013(5) JIS C 0508-1:2012(7)
	使用環境･条件の設定	適切な使用制限が考慮されているかの確認	
	実施体制	危険事象への対応(検知、回避を含む)の主体の確認	
	適切なリスク低減の判断	リスクアセスメント終了の判断方法の確認	
	リスク低減後の再リスク評価	初期リスク評価後、リスク低減方策を考慮した再リスク評価まで実施しているかの確認	

チェックシートの設問趣旨と対応安全規格類(3)

No	設問項目	趣旨	対応規格
Ⅲ	リスク低減手法	リスク低減の方法について準拠している規格・基準の確認	JIS B 9700:2013(5, 6) JIS B 9705−1:2011(4, 5) JIS B 9960−1:2008(6, 9)
	本質的安全化（機器の設計）	設計図面上で改善した機器の仕様や機能の変更の確認	
	本質的安全化（人間工学原則）	人に対する精神的・肉体的ストレスや誤操作の防止が配慮されているかの確認	
	本質的安全化（制御システム）	安全関連部の安全制御のための基本技術が適用されているかの確認	
	本質的安全化（その他の危険源の防止）	電気的・熱的・放射・安定性等の影響に対して設計上配慮されているかの確認	

チェックシートの設問趣旨と対応安全規格類(3)

No	設問項目	基本的リスク低減戦略	対応規格
Ⅲ	保護装置（停止・制動）	緊急停止・保護停止及び制動の実現方法の確認	JIS B 9700:2013(6) JIS B9705−1:2011(4, 5) JIS B 9960−1:2008(6, 9) JIS C 0508−1:2012(6, 7)
	保護装置（動力供給）	動力遮断と蓄積エネルギの消散のために適用される保護方策の確認	
	人体検出時の制御	衝突回避・接触に対するの実現方法の確認	
	付加保護方策	動力源異常時・人の捕捉への対応の確認	
	残留リスク対応	使用上の情報の呈示方法の確認	
	管理	保守・ユーザ教育/資格・廃棄方法の確認	

チェックシートの設問趣旨と対応安全規格類(4)

No	設問項目	設計開発体制、安全監査	対応規格
	組織の構成	組織の明確化、開発フェーズと担当部門間の関連の明確化	
	組織の責任体制	要員の責任･権限の明確化	
	構成メンバー	要員の力量の明確化	
Ⅳ	安全性達成の方針･戦略	安全性に関する方針の提示と周知の確認	JIS C 0508-1: 2012(5, 6, 7, 8)
	組織運営の仕組み	組織内の情報交換の確認	
	文書範囲	必要情報の文書化の確認	
	フェーズ毎の使用技術と方策	各フェーズで必要な技術と方策の明確化	
	以前の勧告、指摘事項	経験の活用と指摘･改善対応の確認	

チェックシートの設問趣旨と対応安全規格類(5)

No	設問項目	趣旨	対応規格
	文書の見易さ	文書管理実施状況、管理ルール	
	文書のタイトル、見出し		JIS C 0508-1: 2012(附属書A) JIS B 9961:2008(10) (参考) JIS Q 9001:2008
	文書作成のルール		
V	版管理	業務全体において、作成、運用される全ての文書に共通の基本要件の確認	
	情報の検索		
	文書範囲		
	改訂、修正、見直し･承認		
	適切な文書管理計画		

チェックシートの設問趣旨と対応安全規格類(6)

No	設問項目		対応規格
Ⅵ	次フェーズに必要な情報	安全関連業務において、必要な情報の文書化の確認	JIS C 0508-1:2012(附属書A) JIS B 9961:2008(10)
	管理情報		
	安全性検証に必要な情報		
	安全性評価に必要な情報		
	安全性評価結果		
	安全性の遂行に必要な業務に関わる文書	安全関連業務において、作成すべき必要文書の確	
	E/E/PE系の安全性の遂行に必要な業務に関わる文書		
	ソフトウェアの安全性の遂行に必要な業務に関わる文書		

安全関連文書、安全関連業務に関する情報

安全管理の運営（開発管理手順、仕様書・計画書・報告書等の文書）を含める予定

コンセプト検証自己チェックシート第1部─安全設計

ロボット介護機器の名称	
型式	

製作者	
シート記入者	
シート記入日	

回答方法
各設問毎に以下の判断基準に従ってチェック欄に✓又は─を記入して下さい（自己判断）。
✓：設問実施済み又は取組中（設問をほぼ満足している又は満足する予定である）
─：設問は該当しない
設問は該当するが、未実施又は検討中の場合はチェック欄は無記入として下さい。
備考欄には補足説明や特記事項等がある場合に記入して下さい。

Ⅰ．安全確保の方針

No	項目	主旨	設問		チェック	備考（補足説明又は該当文書、関連文書の番号）
1	ロボット介護機器の形態	ロボット介護機器の型別の確認（該当機器にチェック）	1	装着型移乗介助機器	✓	
			2	非装着型移乗介助機器	─	
			3	歩行（移動）支援機器	─	
			4	排泄支援機器（トイレ）	─	
			5	見守り用機器	─	
2	安全設計方針	安全に配慮した設計準備の確認	1	安全設計コンセプト又は方針を策定している。	✓	
			2	概略安全仕様を決定している。		
3	人とロボット介護機器の役割	安全確保の主体の確認（安全設計方針として人と対象機器の役割分担の考え方）	1	ロボット介護機器主体 危険事象への対応（検知、回避を含む）は、多くは機器側で対応する。	─	
			2	介護者主体 危険事象への対応（検知、回避を含む）は、多くは介護者側で対応する。	✓	
			3	要介護者主体 危険事象への対応（検知、回避を含む）は、多くは要介護者側で対応する。	─	

Ⅱ．リスクアセスメント

No	項目	主旨		設問	チェック	備考（補足説明又は該当文書、関連文書の番号）
4	リスクアセスメントの基準	準拠している規格・基準の確認	1	リスクアセスメントは関連国際規格又は国内規格に準拠して実施している（規格名を備考欄に記入）。	✓	JIS B 9700:2013
			2	他の規格（社内基準も含む）を参照して実施している（規格名を備考欄に記入）。	―	
5	使用環境・使用条件の設定	対象機器の適切な使用制限が考慮されているかの確認	1	対象機器の基本仕様（動作機能、運用を含む）が決定している。		
			2	対象機器の想定使用環境が明確である。		
			3	対象機器のライフサイクル（寿命）が考慮されている。		
			4	対象機器の想定使用条件（機器に関連する人の属性など）が明確である。		
6	実施体制	チームとして実施しているか、又レビュー後、承認しているかの確認	1	設計者を中心として複数人で実施している。		
			2	結果についてレビューを行っている。		
			3	責任者(チームの管理者など)が最終承認している。		
7	適切なリスク低減の判断	リスクアセスメントの終了の判断方法を定めているかの確認	1	リスク低減目標を具体的に定めている。		
			2	実績のある類似機器等のリスク比較を利用している。		
8	リスク低減後の再リスク評価	初期リスク評価後、リスク低減方策を考慮した再リスク評価まで実施しているかの確認	1	初期リスク評価の結果、リスク低減は不要と判断される。		
			2	リスク低減方策の導入によるリスク低減効果を考慮した再リスク評価を行っている。		

Ⅲ. リスク低減

No	項目	主旨	設問		チェック	備考 （補足説明又は該当文書、関連文書の番号）
9	リスク低減手法	リスク低減の方法について準拠している規格・基準の確認	1	リスク低減は機械安全基本規格（JIS B9700又はISO12100）の3ステップ方式に従って実施している。		
			2	他の規格（社内基準も含む）を参照して実施している（規格名を備考欄に記入）。		
10	本質的安全化（対象機器自体の設計）	設計図面上で改善した対象機器の仕様や機能の変更の確認	1	対象機器の形状に鋭利部、突出部、挟圧部等がない。		
			2	対象機器の部品の材質等が人や環境に影響を与えないよう配慮している。（RoHS対応、ハロゲンフリー等）		
			3	パワー、速度等の性能を必要最小限に制限している。		
			4	その他（防爆構造等）、設計上配慮している（関連項目を備考欄に記入）。		
11	本質的安全化（人間工学原則の遵守）	人に対する精神的・肉体的ストレスや誤操作の防止が配慮されているかの確認	1	対象機器の色、形状などの外観、大きさ、質量（装着型の場合）、構造が人に対して肉体的、精神的ストレスを与えないよう配慮されている。		
			2	マン・マシンインタフェースは、人が誤操作や誤解しないよう配慮されている。		
			3	保守保全作業を含め、無理な姿勢での対象機器操作(人による重量物の扱い、人の動作を極端に規制する装置等）や搭乗姿勢がない。		
12	本質的安全化（制御システムの安全原則の適用）	安全関連部の安全制御のための基本技術が適用されているかの確認	1	制御システムにおいて安全に関連する部分を定義(仕様書等に記載など)している。 （安全部と非安全部が明確に区別されている。）		
			2	制御システムの安全関連部に高信頼化技術（冗長化、多様化を含む）又はフェールセーフ技術を適用している。		
			3	制御システムの安全関連部には、自動監視（自己診断）技術を適用している。		
13	本質的安全化（電気的危険源の防止）	感電や静電気による影響に対して設計上配慮されているかの確認	1	保護特別低電圧（AC25V(実効値)、DC60V以上)以上になる露出部がない。		
			2	金属露出部の絶縁性、耐環境性を配慮している。		
			3	帯電者からの静電気放電による誤動作のないよう配慮されている。		
14	本質的安全化（熱的危険源の防止）	高・低温部が人に及ぼす影響や火災に対して設計上配慮されているかの確認	1	人が触れる可能性のある対象機器の部位には、極端な高温部又は低温部はない。		
			2	対象機器の部品は、想定使用条件下で発火等を起こさないよう選定されている。		
15	本質的安全化（放射による危険源の防止）	音や光等が人に及ぼす影響に対して設計上配慮されているかの確認	1	発生する騒音又は振動は、想定使用条件下で規定されるレベル以下である。		
			2	対象機器周囲へ放射されるレーザ光や超音波等は、人に対して危害を与えない出力である。		
			3	対象機器が発生する電磁気の放射は、想定使用条件下で周囲の人及び電気・電子機器に影響を与えない。		

No.	項目	確認内容		内容		
16	本質的安全化（安定性の確保）	移動・停止・脱着時の使用時安定性に配慮しているかの確認	1	仕様上の移動条件下（最高速度、最高登坂角度、最短転回半径、最大段差等）で転倒しない。		
			2	停止時に転倒しない、又は安定した状態に移行できる。		
			3	対象機器の脱着時に人の動作に支障を及ぼす（バランスを損なう等）ことがない。		
17	本質的安全化（その他）	その他の設計上の配慮の確認	1	他の本質的な安全設計（衛生上も含む）を実施している（具体的な項目を備考欄に記入）。		
18	保護装置（停止の機能）	停止により安全確保するために適用される保護方策の確認	1	人が操作する緊急停止装置を装備している。		
			2	保護停止（インタロックによる停止）機能を有している。		
			3	停止後意図しない起動を考慮している。		
			4	停止以外の方法で安全な状態に移行する（具体的な項目を備考欄に記入）		
19	保護装置（停止方法）	緊急停止の実現方法の確認	1	アクチュエータの動力を遮断して停止する。		
			2	制動して停止後にアクチュエータの動力を遮断する。		
		緊急停止でない場合の停止方法	3	アクチュエータの動力を遮断して停止する。		
			4	制動して停止後にアクチュエータの動力を遮断する。		
			5	制御により停止し、アクチュエータの動力は遮断しない。		
20	保護装置（停止の制御方法）	停止に至るまでの制動の実現方法の確認	1	機械的制動装置により制動する。(ex.機械的ブレーキ、ロック機構等）		
			2	電気的制動機能により制動する。（ex.サーボロック等）		
			3	制動装置・機能は持たずに、制御により減速させる。(ex.速度0制御等)		
21	保護装置（動力供給）	動力遮断と蓄積エネルギの消散のために適用される保護方策の確認	1	アクチュエータの動力遮断後、対象機器の動作を伴わずにエネルギがゼロとなる。(油空圧の残圧、蓄電等の消散)		
22	人体検出時の制御方法	衝突回避の実現方法の確認（アクチュエータを持たない機器又は装着型は原則該当しない）	1	障害物(人を含む)の非接触検知後、制動、停止する。		
			2	障害物(人を含む)の非接触検知後、回避動作をする。		
			3	その他（別の方法があれば備考欄に項目を記入）。		
		接触に対する安全確保方法の確認（アクチュエータを持たない機器又は装着型は原則該当しない）	4	障害物(人を含む)の接触検知後、制動、停止する。		
			5	障害物(人を含む)の接触検知後、回避動作をする。		
			6	接触状態のまま、一定の条件下で動作を継続する。		
			7	その他（別の方法があれば備考欄に項目を記入）。		
		検出情報の通報方法の確認（見守り型の場合）	8	危険状態をアクティブに通報する。		
			9	安全状態をアクティブに通報する。		
			10	対象機器の正常状態を監視・通報できる。		

23	機能安全の配慮	機能安全制御の導入の確認	1	制御システムの安全関連部に安全認証取得済プログラマブル機器を使用している。		
			2	制御システムの安全関連部には機能安全を配慮した設計をしている。		
24	付加保護方策	動力源異常時の対応の確認	1	主動力源異常時は、直ちに停止又は安全な状態へ移行する。		
			2	主動力源異常時は、予備電源に切り替えて一定の条件下で機能を維持する。		
		停止により人が捕捉された時の対応の確認	3	停止時に人が捕捉された場合、手動で脱出又は救助できる。		
			4	停止時に人が捕捉された場合、別動力源により脱出のための動作を行う。		
25	残留リスク対応	使用上の情報の呈示方法の確認	1	対象機器に警報や表示をして、危険情報を人に伝達できる。		
			2	対象機器に警告ラベルを貼付している		
			3	取扱説明書に残留リスクに関する情報を記載している。		
26	管理	対象機器の想定する保守方法の確認	1	ユーザが行うべき保守項目を取扱説明書に記載している。		
			2	ユーザができない保守作業等への対応策が示されている。		
		ユーザへの教育、資格の確認	3	ユーザへ運用に関する教育を行っているか、資格制度を設けている。		
		廃棄対応の確認	4	廃棄方法がユーザに指示されている。		
			5	廃棄は、メーカが引き取って、メーカ責任で行う。		

Ⅳ．安全性の管理

No	項目	主旨	設問		チェック	備考 （補足説明又は該当文書、関連文書の番号）
27	組織構成	開発組織の位置付けの明確化、開発フェーズの流れと担当部門間の相互関係の明確化	1	業務全体の中で、開発フェーズと担当部門が明確になっている。		
			2	業務全体における各フェーズの責任者が規定されている。		
			3	業務全体における各フェーズの入力と出力が明確になっている。		
28	組織の責任および権限	各フェーズに関わる要員の責任と権限の明確化	1	関連する部門や要員の責任と権限が全て規定されている。		
29	構成メンバー	組織にとって必要な力量の明確化	1	要員に必要な力量が明確に規定されている。		
30	安全性達成の方針と戦略	安全性に関する方針を示すことと、その実行意思の伝達の確認	1	安全性の方針が達成されたことを評価・確認することが明確に規定されている。		
			2	安全性の方針は文書化して管理している。		
			3	安全性の方針は関係する要員全てに周知されている。		
31	組織の運営の仕組み	情報が組織内で滞りなく交換されることの確認	1	下部組織の意見・意向などを吸い上げ、活用している。		
			2	業務の有効性について情報交換を行っている。		
32	文書の範囲	必要な情報の文書化の確認	1	安全性の遂行に必要な業務について、文書化する情報の範囲が明確に規定されている。		
33	各フェーズごとに使用する技術と方策	安全性のレベルを確保する方策の確認	1	業務全体における各フェーズに必要な技術と方策が明確に規定されている。		
34	以前の勧告、指摘事項	経験の活用と改善対応の確認	1	過去に開発した安全機能の監査時の勧告、指摘事項の対応を考慮している。		
35	責任ある活動の訓練の手順書	要員が業務遂行に必要な力量を持つこと	1	要員に必要な力量が備わるような教育・訓練計画が作成されている。		
36	部品管理（部品の識別、未認可部品の識別）	必要な部品等の調達間違いの防止	1	部品等の調達についての手順が明確に規定されている。		
37	安全性に関する監査の仕組み	内部監査により、業務のPDCAサイクルと適合性及び有効性を評価	1	監査の計画及び実施、結果の報告、記録の維持に関する手順が明確に規定されている。		
38	監査員の選定（独立性）		1	監査員の（独立性も含めた）資格基準が明確に規定されている。		
39	勧告書の形式		1	監査の計画、実施、結果の報告、対応措置、記録の維持に関する責任並びに要求事項について明確に規定されている。		
40	変更・変更許可の仕	不適合に対する管理の詳細や責任の所在の明確	1	不適合を、どのように識別、評価、処置し、関係会社、関係部門へ連絡するかの手順が明確に規定されている。		

	組み	任の所在の明確化	2	不適合が修正された場合、要求事項に適合するかを再検証している。		
41	情報管理の仕組み	情報管理の確認	1	設計・開発時における危険源や安全関連情報を管理する仕組みがある。		
42	進行状況の管理	責任者による業務進行管理の確認	1	業務の経過を監視・測定する手順が明確に規定されている。		
43	見直しの仕組み・デザインレビュー	変更に対する検証と妥当性確認	1	設計・開発の変更の手順が明確に規定されている。		
			2	使用する文書を常に現在有効な版に保つための更新時の手順が明確に規定されている。		
44	担当者の責任担当者への役割、責任の通知	要員の責任と権限の決定と各要員による理解	1	規定された運用に関連する部門や要員の責任と権限(体制)を、関連する全ての要員に周知している。		

Ⅴ．文書の管理（一般）

No	項目	主旨	設問		チェック	備考（補足説明又は該当文書、関連文書の番号）
45	文書の見易さ	業務全体において、作成、運用される全ての文書に共通の基本要件の確認	1	文書は見易い構成になっている。		
			2	文書は、正確、簡潔である。		
			3	文書は目的に沿っており、理解し易い。		
			4	文書は保全し易い。		
46	文書のタイトル、見出し		1	文書には内容の範囲が分かるような表題や見易いタイトル、小見出しがつけられている。		
			2	経時的変化、変遷に対応している。		
47	文書作成のルール		1	文書作成手順、保管手順（保管場所、保管責任者、保管期限、持ち出し、閲覧）がある。		
			2	文書が改訂された際、関連する全ての部門への配付管理に関する手順がある。		
48	版管理		1	文書の変更の識別及び現在有効な版の識別が確実にできるようになっている。		
49	情報の検索		1	文書は関連情報の検索ができるように構成されている。		
50	改訂、修正、見直し・承認		1	文書の改訂、修正及び見直し手順がある。		
51	適切な文書管理計画		1	業務において関連する全文書を明確にして、文書の改訂、承認などの手順に従って適切に管理している。		

Ⅵ. 安全関連業務に関わる文書

No	項目	主旨		設問	チェック	備考 （補足説明又は該当文書、関連文書の番号）
52	次フェーズに必要な情報	安全関連業務において、必要な情報の文書化の確認	1	安全性の遂行に必要な業務の各フェーズにおいて、次のフェーズへ引き渡す情報を文書化している。		
53	管理情報		1	安全性の管理に必要な情報を文書化している。		
54	安全性検証に必要な情報		1	安全性の遂行に必要な業務の各フェーズにおいて、設定目標未達成時の処理後に行う検証に必要な情報を文書化している。		
55	安全性評価に必要な情報		1	安全性の仕様を定性的、定量的に表現して文書化している。		
56	安全性評価結果		1	安全性の評価から得られる情報と結果について文書化している。		
57	安全性の遂行に必要な業務に関わる文書	機能安全設計で必要とされる基本関連文書の確認 （機能安全に限らず安全設計一般として必要）	1	概念に関する説明書		
			2	全ての適用範囲の定義に関する説明書		
			3	危険源及びリスク解析に関する説明書		
			4	全ての安全要求事項（安全機能、安全度水準を含む）に関する仕様書		
			5	安全要求事項の割り当てに関する説明書		
			6	全フェーズの安全性に関する計画書		
			7	全フェーズの検証に関する計画書		
			8	全フェーズの機能安全評価に関する計画書		
58	電気・電子プログラマブル電子系の安全性の遂行に必要な業務に関わる文書	機能安全設計ベースで要求される詳細関連文書の確認 （機能安全設計の場合に該当）	1	全ての安全要求事項（安全機能、安全度水準を含む）に関する仕様書		
			2	妥当性確認に関する計画書		
			3	ハードウェア及びソフトウェアアーキテクチャ設計に関する計画書		
			4	ハードウェアアーキテクチャ設計に関する説明書		
			5	ハードウェアアーキテクチャ統合テストに関する仕様書		
			6	ハードウェアモジュール計画に関する仕様書		
			7	ハードウェアモジュールテストに関する仕様書		
59	ソフトウェアの安全性の遂行に必要な業務		1	ソフトウェア安全要求事項（安全機能、安全度水準を含む）に関する仕様書		
			2	妥当性確認に関する計画書		
			3	ソフトウェアアーキテクチャ設計に関する説明書		
			4	ソフトウェアシステム設計に関する説明書		
			5	ソフトウェアシステム統合テストに関する仕様書		
			6	ソフトウェアモジュール設計に関する仕様書		
			7	ソフトウェアモジュールテストに関する仕様書		